# Claims

[c1] What is claimed is:

1.A method to prevent illegal copying of an electronic document in a computer system, the computer system comprising a server for connecting to a plurality of terminals via a network, each terminal having a terminal identification code for identifying the terminal, each terminal capable of requesting an electronic document from the server via the network, the server capable of encrypting original plaintext of the electronic document to a corresponding ciphertext, the ciphertext capable of being transmitted to the terminal via the network and being decrypted to the original plaintext, the method comprising a registration process and a document request process, the registration process comprising:

installing a reading application program in a terminal, the reading application program comprising a first secret key;

utilizing the reading application program to register the terminal with the server;

encrypting and transmitting to the terminal a user identification code and a second secret key, the user identification code and the second secret key being generated by the server; and

generating a terminal encryption file by encrypting the user identification code, the second secret key, and the terminal identification code, the terminal encryption file being stored in the terminal;

the document request process comprising:

a terminal requesting the server for an electronic document, the server using the second secret key to encrypt plaintext of the electronic document to corresponding ciphertext, the ciphertext being transmitted to the terminal via the network;

using the first secret key to decrypt the terminal encryption file to retrieve the second secret key and the terminal identification code; and

utilizing the retrieved second secret key to decrypt the received ciphertext if a run-time terminal identification code corresponds to the terminal identification code retrieved from the terminal encryption file, otherwise terminating further decryption to prevent illegal copying of the electronic document by unregistered terminals.

[c2] 2.The method of claim 1 wherein the terminal further comprises a central processing unit (CPU), a hard-disk, and a network card, and the terminal identification code is selected from one of an identification code from the CPU, the hard-disk, or the network card.

[c3] 3.The method of claim 1 wherein the server comprises a user database for recording a plurality of user identification codes of registered users, and terminal identification codes.

[c4] 4.The method of claim 3 wherein the server comprises a secret key generating module for generating a second secret key for each user registered in the user database.

[c5] 5.The method of claim 4 wherein the server comprises a key database for recording the user identification codes of the registered users, and the associated second secret keys.

[c6] 6.The method of claim 1 wherein the server comprises an encryption module for encrypting and transmitting to the terminal the second secret key and the user identification code.

[c7] 7.The method of claim 6 wherein the server comprises an electronic document database for storing associated plaintexts of a plurality of electronic documents, and a control center for controlling operations of the server.

[c8] 8.The method of claim 7 wherein when the server receives a request for the electronic document by the terminal, the control center locates the associated plaintext of the electronic document, and the encryption module encrypts the plaintext of the electronic document with the second secret key to form the corresponding ciphertext.

[c9] 9.The method of claim 1 wherein the first secret key and the second secret

key are both 128-bit encryption keys..

[c10] 10.The method of claim 1 wherein the server comprises a public software module for storing the reading application program to be downloaded to the terminals by users.

[c11] 11.A computer system to prevent illegal copying of an electronic document, the computer system comprising a server for connecting to a plurality of terminals via a network, each terminal having a terminal identification code for identifying the terminal, the terminals capable of requesting an electronic document from the server via the network, the server capable of encrypting original plaintext of the electronic document into a corresponding ciphertext, the ciphertext being transmitted to the terminal via the network and being decrypted to the original plaintext, the server comprising:
a public software module for storing a reading application program to be downloaded to the terminals, the reading application program comprising a first secret key;
a registration module, capable of generating a user identification code on registration of a terminal;
a secret key generating module for generating a second secret key specified for a registered user; and
an encryption module capable of encrypting and transmitting the user identification code and the second secret key transmitted to a registered terminal;
wherein when the reading application program of the terminal receives the user identification code and the second secret key, a terminal encryption file is generated by encrypting the user identification code, the second secret key and the terminal identification code, and the terminal encryption file is stored in the registered terminal wherein when a terminal requests the server for an electronic document, the encryption module encrypts plaintext of the electronic document as the corresponding ciphertext with the second secret key, and the ciphertext is transmitted to the terminal via the network, and when the reading application program of the terminal receives the

ciphertext, the first secret key is used to decrypt the terminal encryption file to retrieve the second secret key and the terminal identification code,and when the reading application program identifies a run-time terminal identification code that matches the terminal identification code retrieved from the terminal encryption file, the retrieved second secret key is used to decrypt the received ciphertext, otherwise, further decryption is terminated to prevent illegal copying of the electronic document by an unregistered terminal.

[c12] 12.The computer system of claim 11 wherein the terminal further comprises a central processing unit (CPU), a hard-disk, and a network card, and the terminal identification code is selected from one of identification codes from the CPU, the hard-disk, or the network card.

[c13] 13.The computer system of claim 11 wherein the server comprises a user database for recording a plurality of user identification codes of the registered users and the associated terminal identification codes.

[c14] 14.The computer system of claim 11 wherein the server comprises a key database for recording all the registered users and the specified second secret keys.

[c15] 15.The computer system of claim 11 wherein the server comprises an electronic document database for storing the plaintext of the plurality of electronic documents, and a control center for controlling operations of the server.

[c16] 16.The computer system of claim 15 wherein after receiving a request for an electronic document by a terminal, the control center of the server locates the plaintext of the electronic document, and the encryption module encrypts the plaintext of the electronic document with the second secret key to form the corresponding ciphertext.

[c17] 17. The computer system of claim 11 wherein the first secret key and the second secret key are both 128-bit encryption keys.